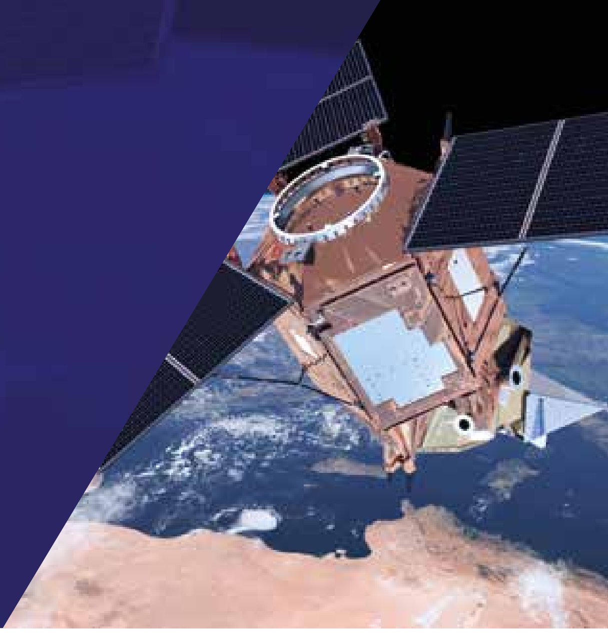
USE CASE

GUARANTEEING THE CONFIDENTIALITY OF EXCHANGES

Case of an independent subsidiary of a major European space technology company



This company supplies major State players and international private companies with its products and services.

REQUIREMENTS

The chosen solution must **secure all information exchanged by e-mail** whenever the sender considers that the exchanged information is sensitive, regardless of the recipients, including external contacts. **Only the sender and the recipients must be able to decipher and read it,** including **when on the move**, and **on any terminal.**

The solution must also:

+ Be as transparent as possible for the user;
+ Be administrable and capable of **applying a Corporate Security Policy**
Lastly, since the information handled may be marked **Restricted,** the product must be approved to protect this type of data.

SOLUTION

The customer chose the **ZED!** and **ZEDMAIL** solutions for their project and deployed them on **all their workstations.** All external contacts are also invited to procure one of these solutions, or else the free multi-platform add-on **ZEDFREE,** which makes it possible to decipher and respond in encrypted format. This add-on is available on Windows, MacOS, Linux, Android and iOS.

EXPERIENCE

IT

Plug-in for MS Outlook™, mastered and deployed by Microsoft remote software deployment tools.

USERS

One click to encrypt, two clicks to decrypt.

INFORMATION SYSTEM SECURITY

Definition of the contexts in which all exchanges must be encrypted.

BENEFITS

The chosen solutions enable **end-to-end protection** to be set up from any type of terminal, including mobile terminals. In this way, they guarantee **complete partitioning of information** even internally.

ZED! is also an **EAL3+ CC certified product with Standard Level qualification** from the **ANSSI** (French national agency for information system security) and is authorised to protect information marked **NATO / EU Restricted,** thus meeting the need to protect information at the Restricted level.

These encryption solutions do not require the integration of a key management infrastructure. Furthermore, in accordance with their requirements, **password keys,** the complexity of which is imposed by the company, can be used with the chosen solutions.

NEXT STEPS

Passwords will be replaced by certificates for internal e-mail encryption when the next PKI is deployed.

ZEDMAIL

ZED!

PRIMX
MAKE ENCRYPTION HAPPEN